AMENDMENTS TO THE SPECIFICATION

Please replace Paragraph **[0002]** with the following paragraph rewritten in amendment format:

[0002] With the explosion of the Internet, the number of available Internet Protocol version 4 (IPv4) addresses are insufficient to meet the demand. Although an IP version 6 network architecture has been proposed to deal with the address shortage, IPv4 remains prevalent. Network ~~address translation~~ Address Translation (NAT) is one approach that helps solve the address shortage in the IPv4 environment, but it brings challenges and difficulties for certain applications.

Please replace Paragraph **[0003]** with the following paragraph rewritten in amendment format:

[0003] In general, a NAT capable device maintains a private network and translates private network host addresses to certain public addresses when these hosts are communicating with public network hosts. However, it introduces complications to many applications. For example, a host in the public domain is not able to initiate a TCP connection to a host behind a NAT router. Although this ~~could bring~~ has some security value, it brings inconvenience to ~~peer to peer~~ peer-to-peer applications. One such application is IP telephony, where ~~either the~~ ITU H.323 signaling and/or ~~the~~ Real-time Transport Protocol (RTP) streams may encounter problems with NAT routers. As Internet applications continue to ~~grow exponentially~~ develop, it becomes more and more important ~~difficult for vendors~~

~~to adapt to various peer to peer applications, and yet it makes application development difficult without resolving the~~ to be able to traverse NAT ~~traversal issue~~ systems.

Please replace Paragraph **[0004]** with the following paragraph rewritten in amendment format:

[0004] The present invention proposes a new framework and mechanism for a NAT router ~~which~~ to support ~~supports~~ peer-to-peer applications. The framework is compatible with existing IP routing and network address translation mechanisms, and allows IP networks to be extended to support new applications.

Please replace Paragraph **[0012]** with the following paragraph rewritten in amendment format:

[0012] Figure 5 is a flowchart depicting an exemplary routing protocol performed by a router for data packets being sent to a network device residing in a private network in accordance with the present invention; and

Please replace Paragraph **[0013]** with the following paragraph rewritten in amendment format:

[0013] Figure 6 is a diagram illustrating the operation of the exemplary routing protocol shown in ~~Fig.~~ Figure 5 in accordance with the present invention.

Please replace Paragraph **[0014]** with the following paragraph rewritten in amendment format:

[0014] A ~~network address translation~~ Network Address Translation (NAT) mechanism brings both the advantage of extending the IP network address space[[,]] and the ~~difficulties~~ difficulty of ~~to~~ implementing peer-to-peer network communications due to the NAT mechanism's use of non-routable private IP addresses. Therefore, the present invention defines [[an]] a hierarchical addressing mechanism which allows global identification of ~~any~~ hosts that are connected to the public ~~internet~~ Internet through specially configured router devices. This scheme is referred to as a "traversable hierarchical IP addressing scheme."[[.]] This addressing scheme considers almost all possible ~~internet~~ Internet connection types[[:]], including ~~host~~ hosts directly connected to the Internet with a public IPv4 address[[;]] and ~~host~~ hosts in a private network ~~which is~~ connected to the public Internet ~~with~~ via one or more routing devices.

Please replace Paragraph **[0015]** with the following paragraph rewritten in amendment format:

[0015] The proposed addressing scheme uses existing addresses that hosts have been assigned, and therefore requires no new address assignment ~~and~~ or allocation scheme. In general, consider that any host that connects to the Internet has a unique ~~traversable hierarchical IP address~~ Traversable Hierarchical IP Address (THIA), which is composed of ~~addresses of~~ the host's

existing allocated IP address[[,]] and the public network interface address of routing devices interposed between the host and a public network.

Please replace Paragraph **[0016]** with the following paragraph rewritten in amendment format:

[0016] Referring to Figure 1, suppose an exemplary host 12 is assigned with a private IP address of 192.168.1.25, and that there are two exemplary routers cascaded [[in]] between this host 12 and the Internet. The router directly connecting to the Internet has ~~the~~ an address of 208.151.56.123 ~~for~~ as its public side network interface, while the other ~~one~~ router has ~~the~~ an address of 10.1.10.2 as its public side network interface address. ~~Then, define the~~ The host's THIA is defined to be the ordered concatenation of the three addresses. For clarity ~~reason~~, the host's THIA is notated as the three addresses concatenated ~~to each other~~ with a colon ~~as a~~ separator as follows: "208.151.56.123:10.1.10.2:192.168.1.25". As shown, the THIA begins with the public interface address of the ~~outer most~~ outer most router and ends with the host's private assigned address.

Please replace Paragraph **[0017]** with the following paragraph rewritten in amendment format:

[0017] More formally, the THIA is defined to be an integer ~~with~~ whose length ~~to be~~ is a ~~muliple~~ multiple of four bytes, every four consecutive bytes ~~corresponds~~ corresponding to an IPv4 address of a device. The THIA is formed

in a predefined order so that it reflects the order of the cascaded (if any) routers. In the example above, the outer most router is at the beginning and the host device is at the end. Notation for the THIA uses the traditional IPv4 address notation with colons separating different devices' IP addresses.

Please replace Paragraph **[0018]** with the following paragraph rewritten in amendment format:

[0018] Figure 2 depicts a packet header 20 in accordance with the Internet Protocol (IP). The packet header is generally comprised of multiple 32-bit words. A minimum length packet header is comprised of five 32-bit words, including a source IP address field 22 and a destination IP address field 24. ~~However, an option exists within the~~ The header ~~which~~ allows for ~~further~~ optional bytes to be added in an options field 26 of the packer header. An IP header length field 28 dictates the number of ~~the~~ optional bytes. Since the IP header length field is a 4 bit number, this implies that the options field may be as long as ten 32-bit words. As further described below, hierarchical network addressing information may be embedded into the options field 26 [[on]] of an IP packet header in accordance with the present invention. While the following description is provided with reference to the Internet Protocol, it is readily understood that the present invention is suitable for other types of networking protocols ~~which have the capability of adding optional bits of information into the data packet~~.

Please replace Paragraph **[0019]** with the following paragraph rewritten in amendment format:

[0019] Network ~~address translation~~ Address Translation (NAT) is typically performed by a router ~~which~~ that sits between a private network and a public network[[,]] such as the Internet. In operation, the router is configured to translate an unregistered private IP address which resides on the private network to a globally unique, registered IP address. However, an improved protocol is provided for routing data packets using traversable hierarchical network addressing. Unless explicitly stated, the routers or network routing devices in this document refer[[s]] to the class of routers with ~~address translation~~ NAT functionality.

Please replace Paragraph **[0020]** with the following paragraph rewritten in amendment format:

[0020] Figures 3 and 4 illustrate a routing protocol for data packets being sent from a source host 42 residing in a private network. Initially, data packets are formulated by the source host 42. For instance, the source IP address field of the packet header is formatted with a private IP address 43 for the originating host device 42, and the destination IP address field of the packet header is formatted with a destination IP address 45.~~; it~~ It is understood that the remainder of the data packet[[s]] is also formulated in accordance with the Internet Protocol.

Please replace Paragraph **[0022]** with the following paragraph rewritten in amendment format:

[0022] The options field may be defined to include two types of options: a source address option and a destination address option. Either option may further include a flag byte (octet), a length byte (octet), and one or more IP addresses. Multiple addresses are concatenated together as further described below. It is ~~readily~~ understood that the source address option and the destination address option may use different flag values.

Please replace Paragraph **[0024]** with the following paragraph rewritten in amendment format:

[0024] To the extent that multiple routers are interposed between the originating host and the public network, it is readily understood that this process is repeated for each intermediate routing device. In other words, the IP address is extracted from the source IP address field of the packet header and appended to the address information residing in the source address option of the packet header at each router. In addition, the source IP address field is reformatted with the public interface IP address for the given router. Each time a router updates the options field, the packet header is updated accordingly, including the length byte in the source address options. When the data packet is finally sent to the public network, it is readily understood that the source address option is formatted with an IP address for the source device followed by IP addresses for ~~the~~ each intermediate routing device ordered in an inner to outer sequence, and

the source IP address field is formatted with the public interface address for the outer most router associated with the private network. Thus, each packet header contains source address information that enables peer-to-peer communication with the source host.

Please replace Paragraph **[0026]** with the following paragraph rewritten in amendment format:

[0026] Figures 5 and 6 illustrate a routing protocol for data packets being sent to a destination host 62 having a private IP address and residing in a private network. For discussion purposes, it is assumed that the destination host IP address is known to the source host 66, and thus is embedded in the data packets being sent to the destination host 62. In one exemplary embodiment, the IP address of the destination host may have been learned in the manner described above. In another exemplary embodiment, the destination host may have registered its ~~tranverable~~ traversable hierarchical network address at a ~~domain name server~~ Domain Name Server (DNS). Knowing a peer station name, the source host may send a DNS query to retrieve the ~~tranversable~~ traversable hierarchical network address of the destination host. ~~However, it is envisioned that other~~ Other techniques for learning the destination host IP address are also within the scope of the present invention.

Please replace Paragraph **[0027]** with the following paragraph rewritten in amendment format:

[0027] First, the source host 66 must format the packet header with the applicable destination address information. The destination address information is also embedded into the options field of the packet header in a manner as described above. In particular, the options field may include a destination address option. The destination address option is further defined to include a flag byte (octet), a length byte (octet) and one or more destination IP addresses. The destination addresses are concatenated together, such that the public interface address for the second most outer router is at the beginning of the address field (i.e., top of the stack) and the private IP address for the destination host device is at the end of the address field (i.e., bottom of the stack). In other words, the destination addresses are ordered in an outer to inner manner in relation to the public network. However, it is to be understood that the address information may be ordered in any predefined manner known to the network devices. It is also readily understood that the public interface address for the outer most router is inserted into the destination IP address field of the packet header. Formatted data packets are then sent by the source host 66.

Please replace Paragraph **[0030]** with the following paragraph rewritten in amendment format:

[0030] To the extent that multiple routers are interposed between the public network and the destination host, it is ~~readily~~ understood that this process [[is]] can be repeated at each intermediate routing device. In other words, the destination IP address is extracted from the destination address option and

inserted into the destination IP address field of the packet header. When the data packet is finally sent to the destination host, it is ~~readily~~ understood that the destination IP address field is formatted with the private IP address for the destination host. Thus, the data packet was routed in a peer-to-peer manner from the source host to the destination host.

Please replace Paragraph **[0033]** with the following paragraph rewritten in amendment format:

[0033] In response to an address query message, the network routing device sends a reply message to the requesting device which contains its traversable hierarchical network address. As previously discussed, a traversable hierarchical network address includes the public interface IP address for the responding network routing device prepended with public interface IP addresses for any other network routing devices interposed between the responding network routing device and the public network. In one embodiment, the responding network routing device may be configured to use the same protocol to discover the public interface IP addresses of any other network routing devices interposed between the responding network routing device and the public network. Alternatively, the network routing devices may be configured to multicast through its private side interface a notification message that contains its public interface IP address, so that other network devices may learn its address without sending a query message. The notification message may be sent when the device is first powered on or at ~~period~~ periodic time intervals.